

Monthly Publication: Information Security, Taiwan (circulation: 10,000/ October 2008)

Present and Future Outlook for the Network Security Industry

With network threats gaining sophistication and demands for network applications changing rapidly, security vendors reach by launching new products with a shorter time-to-market.

According to Spencer Chen, Country Manager of Fortinet Taiwan, there is still a big opportunity in the UTM market. In addition, Fortinet has just acquired IPLocks and entered the database security market with FortiDB, its new database security appliance. The company has also improved its content processor to enable better small-packet filtering. Currently, all Fortinet UTM appliances use FortiASIC CP6 processor, including FortiGate-310B, which was launched in Q4 for the Taiwanese market.

網路安全產業的 現在與未來

隨著資安威脅不斷演進與企業對網路應用需求的改變，安全廠商推出新品的速度也越來越快，且看各廠如何突顯自家優勢、如何走下一步棋。

文 | 張維君

只要公司營運穩定，ERP系統一用可以數年不需改變。然而網路安全產品的使用年限約莫只有3至5年，因此汰換時期一到，常見各家廠商市場版圖大搬風。

UTM市場穩定成長

網路安全領域這幾年來流行著不同的解決方案。早期談縱深防禦，企業在內網骨幹重兵佈署各種防禦設備，防火牆、入侵偵測、郵件過濾等系統，而整合威脅管理(UTM)系統於2004年IDC下了明確定義後也成為市場顯學。雖然一直以來功能全開、效能不彰等問題深受企業詬病，但在原廠技術突破與經銷通路的努力下，UTM市場成長力道仍然不容小覷。

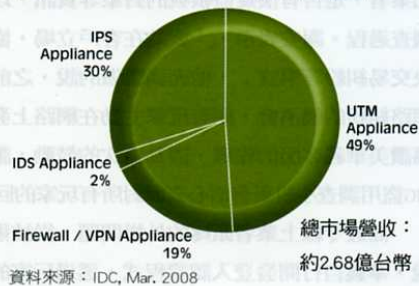
根據IDC 2007年第四季度資訊安全硬體裝置追蹤季報顯示，台灣資安硬體裝置市場營收達838萬美元，其中UTM佔49%，因為政府及國防單位的專案釋出，甚至表現出51.98%的YoY強勢成長。另一方面，也可見網路安全供應端對UTM產品不管是高階、中低階機型均陸續有新品推出。

從軟體走向硬體發展的Check Point 亞太區副總裁Itzhak Weinreb持續看好UTM市場，認為隨企業擴展，IT新技術的帶動，企

業對UTM仍會有汰舊換新的需求。現階段Check Point所推出UTM產品已往下延伸到中小企業市場，然而許多中小企業預算有限，因此Check Point市場策略會傾向與電信業者合作，以月付費用的方式提供中小企業一條乾淨的網路線。

Juniper先進技術資深經理林信駿表示，隨新興IT技術的推出，將來Juniper的所有設備會往更高Throughput支援。他認為，當資安變成企業IT基礎架構時，安全是加在路由器、交換器之上而且不犧牲效能。近期推出的SRX動態服務閘道器即強調功能全開效能不減。「既是大型UTM，也是兼具安全功能的Core Switch。」他說。

4Q 2007台灣資安硬體裝置市場營收分佈圖



許多廠商都看到此波網頁掛馬防護需求，也投入在閘道過濾技術的提升並試圖解決效能問題。

Fortinet台灣區總經理陳鴻翔以第二代防火牆的概念來推廣UTM。陳鴻翔指出，由於防毒牆效能不彰，最多只能撐400~500Mbps，且很耗資源，所以把UTM當作防火牆加防毒閘道來推，市場接受度很高。十分看好防毒牆市場的他表示，許多企業僅在伺服器端安裝防毒軟體，沒有在閘道端做，這塊市場商機仍然很大。

今年年初以來威脅轉向網頁掛馬，網頁掛馬的最終目的為了入侵用戶端。許多廠商都看到此波防護需求，也投入在閘道過濾技術的提升並試圖解決效能問題。這塊市場除網頁應用安全廠商外，擁進防毒軟體、URL過濾、廣域網路優化廠商...等業者。Websense日前推出新版Web Security Gateway除了新增對Web 2.0網站上圖片、字體、標題等網頁元件的過濾之外，透過ThreatSeeker技術，其Active Security Module可即時分析網頁script，偵測惡意軟體。同樣採取Proxy mode的BlueCoat，在其WebFilter上的WebPulse service則是採用雲端運算技術，結合社群力量過濾問題網頁，在閘道端模擬PC瀏覽器使用環境以偵測網頁內藏的問題。

中央控管化繁為簡

除了閘道防毒之外，端點安全、網路存取控制(NAC)是另一發燒議題。根據去年底本刊所做的調查，NAC是許多大廠今年看好的市場。由於企業網路邊界逐漸模糊，攻擊除了從閘道而來，防禦能力薄弱的端點也成為攻擊標的。至於在解決方案方面，防毒軟體業者、網路設備業者均有產品推出。林信駿認為，大家不想被單一廠商設備綁住，架構能否夠彈性是企業評選的關鍵。再加上許多企業想在內網實施政策執行(policy enforcement)的地方都不一樣，「有些希望管到枝微末節的地方去」，而Fortinet自推出首個有NAC概念的產品FortiGate 224B後，有感於對其他安全產品的整合度會是NAC的關鍵，因此市場策略已略有轉向。

端點安全許多人朗朗上口，但廠商們卻有不



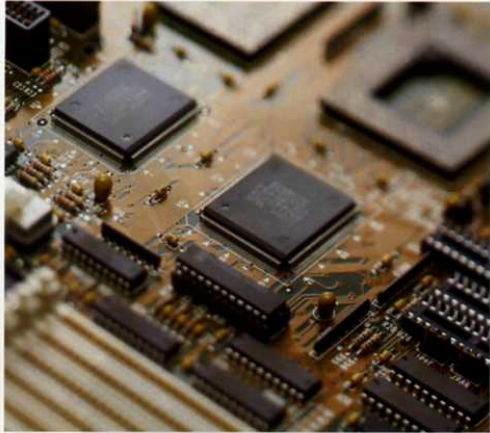
Check Point將透過購併等方式
取得端點安全其他新技術。

Check Point亞太區副總裁Itzhak Weinreb

同定義。Weinreb表示，Check Point是以資料加密的角度出發，相對於其他防毒軟體廠商所談的端點安全而言，現階段網路安全的解決方案已近於完整。Check Point接下來產品發展的重心會在端點安全的部份，包括透過購併的方式取得一些技術。

當企業越來越清楚網路安全是層層堆疊上去，也能接受閘道防毒、伺服器防毒等觀念時，管理方便性成為新的議題。

CheckPoint以單一代理程式簡化所有CheckPoint產品管理。在購併PointSec之後的端點安全產品也快速地完成整合，可透過SmartCenter集中管理。CheckPoint台灣區總經理簡淑真表示，許多客戶反映的需求是必須管理很多套系統，因此特別強調做到簡化管理。Juniper的NSM中央控管平台，使網管與資安管理工作整合後達到1加1大於2的綜效。林信駿說，大型企業網管與資安通常分別由不同組負責，過



▲ 網路安全廠商不斷尋求技術突破，往更高效能支援。

去為了提升防護等級，設定了安全政策就難免影響網路效能。兩組人員在績效上相互抵觸競爭，許多工具的佈署其實是疊床架屋。NSM將其整合之後即能做到效能與安全兼具。

洞燭先機的下一步

從UTM 闖道防毒到NAC，下一步各大廠商又看到不同新趨勢，紛紛搶先卡位以掌握領先技術。

Check Point為行動安全商機做準備

看好未來對於行動設備的安全上網需求，Check Point準備加入行動安全防護戰局，推出以flash device的設備內建虛擬桌面應用程式，直接提供行動商務人士安全連線存取企業內部網路的資源，以做到更全面的行動安全。

Juniper看好SIEM

今年初以模組化方式推出的STRM安全事件管理系統(SIEM)。林信駿認為，由於產品採漸進式模組化架構，可先做日誌管理再做關聯分析，且不同於其他以介接網路設備數目來計價的方式，企業接受度高。預計年底將再推出智慧型新版本，可做到依據事件分析結果，自動reconfig路由器等網路設備。

Fortinet押寶資料庫安全

自今年年中宣佈買下資料庫安全廠商IPLocks之後，產品整合進度快速。今年4Q即將宣佈推出FortiDB，而台灣也準備在明年1Q問市。看好將受法規帶動資料庫安全市場的需求，FortiDB將以硬體裝置推出來解決過去IPLocks以軟體方式所遭遇的效能問題。除新產品線FortiDB外，在UTM硬體效能方面也將有突破。推出ASIC CP6第6代網路處理器，使UTM不需要過於依賴CPU，能以不同的引擎處理更多流量，尤其在對小封包的過濾處理上將有改善。減少掉封包的問題。即將在4Q推出的FortiGate310B也將採用此款晶片。

BlueCoat喊出直接連網

產品定位特殊，與其他網路安全產品市場部分重疊卻無直接衝突的BlueCoat。將與安全大廠同時維持合作與競爭關係。除了持續採取平台概念引進不同供應商提供選擇，防毒部份提供Panda、McAfee、Sophos、Kaspersky等4種引擎；在網頁過濾部份同時有自己的也支援Websense資料庫；而防止資料外洩的部份也支援Port Authority（Websense購併）、Vontu（賽門鐵克購併）、Reconnex、Vericept、Code Green等。台灣區總經理張元正表示，預計未來會增加支援更多廠商。

綜上所述，網路安全威脅的演變，各大廠商所關注到的需求與採取的產品策略其實大同小異。例如強調中央控管平台時，各家所專注就是報表管理能力，如何將報表更精緻化等。然而企業必須清楚的是，以產業生態來說，許多經銷通路眼裡只有容易銷售的產品，但這些工具進來是否真能發揮最大效益，是否真能提升防禦等級，解決方案能做到的恐怕有限。企業也許需要同時思考人員、流程面的解決之道，才不會買了IPS不去看Log分析，又得另外買SIEM來分析，讓管理階層留下資安就是一堆花錢的印象，資安產品又背負ROI低的黑鍋。 i